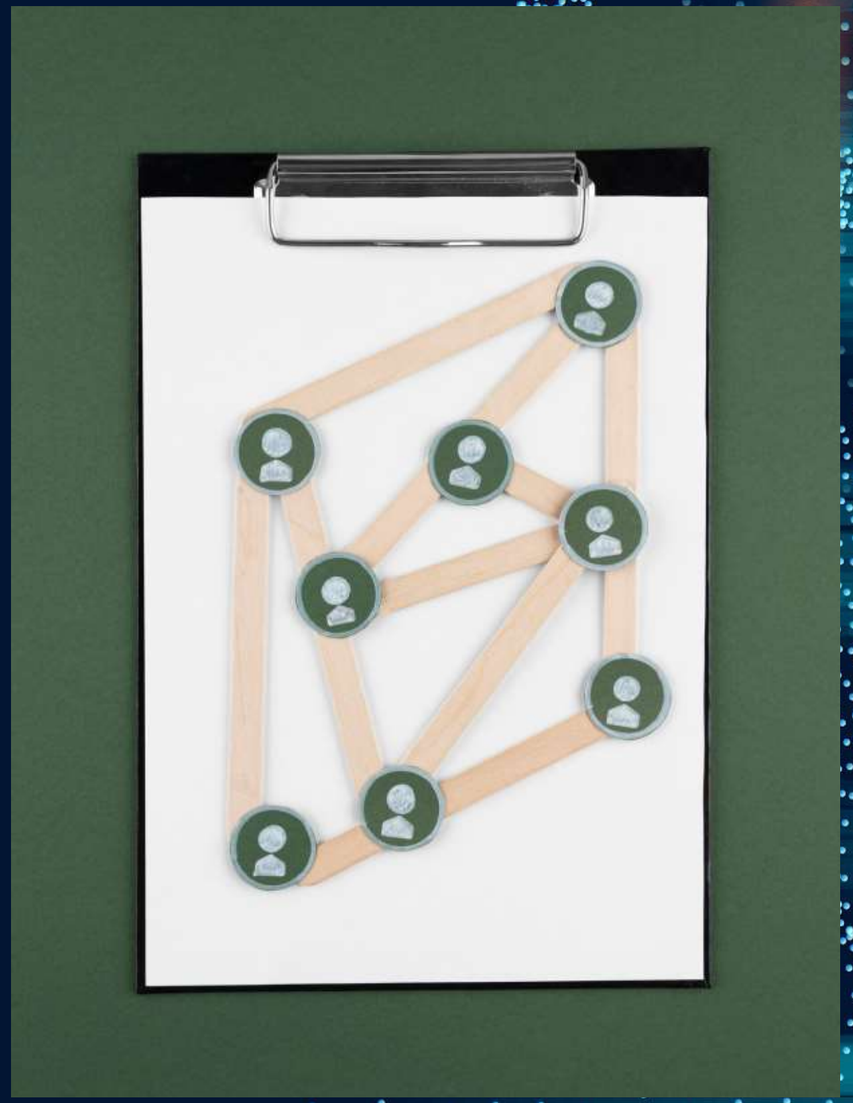
# SMART INDIA HACKATHON 2024

TITLE PAGE

- **Problem Statement ID – 1559**
- **Problem Statement Title-** ***Develop a functional solution that demonstrates the hardware enabled root of trust.***
- **Theme-** ***Smart Automation***
- **PS Category-** ***Hardware***
- **Team ID -**
- **Team Name (Registered on portal) -** ***Secura***

# Problem Overview

Develop a platform-agnostic solution (Android/iOS) for UIDAI that uses hardware-generated key pairs linked to the device's IMEI. The private key must remain in the hardware enclave for secure, offline encryption, supporting key lifecycle management (expiry/revocation) without backend reliance.



# SECURA

Trust built into every device !

# What is SECURA?

1.Secura is a hardware-enabled security solution designed to establish a root of trust.

2. Demonstrates vulnerabilities in traditional app-controlled systems.

3. Highlights secure alternative using hardware-backed encryption.

# Key Objectives of SECURA

1. Secure key generation and storage within hardware (enclave).

2. Platform-agnostic (works on both Android and iOS).

3. Offline functionality with no reliance on backend servers.

4. Use of RSA PKCS/OAEP encryption protocols.

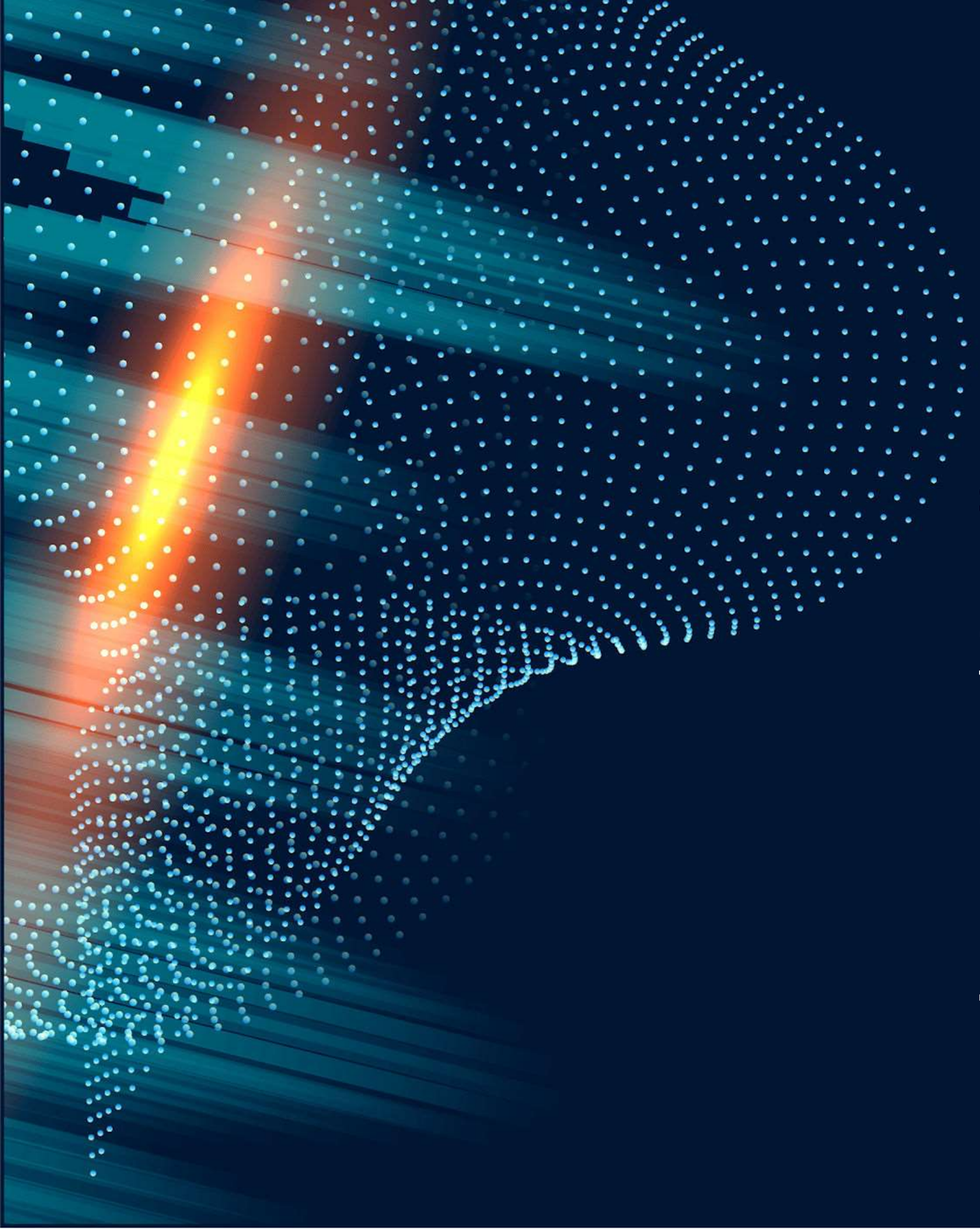
5. Key lifecycle management (generation, expiration, and revocation).

# Insecure Setup Demonstration

L. A generic mobile app controls an LED and a lock.

2. Vulnerabilities: easily manipulated by unauthorized users.

3. No hardware-based protection for encryption or key management.



# Secura Setup Demonstration

1. Secura uses hardware-backed key pairs stored in a secure enclave.

2. Only authorized access is possible through the custom Secura app.

3. Key pairs tied to the device’s unique identifier (e.g., IMEI).

4. Demonstrates secure control over the LED and lock.

# Understanding the Root of Trust

The root of trust is a hardware-based security anchor.

Ensures private keys are generated and stored within secure hardware.

Cryptographic operations (encryption, decryption) happen inside the enclave.

Protects against unauthorized access and tampering.

# Key Lifecycle Management

- Key Generation: Generated in secure hardware (enclave).
- Key Usage: Tied to specific device components (e.g., locks, LEDs).
- Key Expiration: Keys can be set to expire after a certain period.
- Key Revocation: Keys can be revoked in case of a security breach.


# Offline Security Features

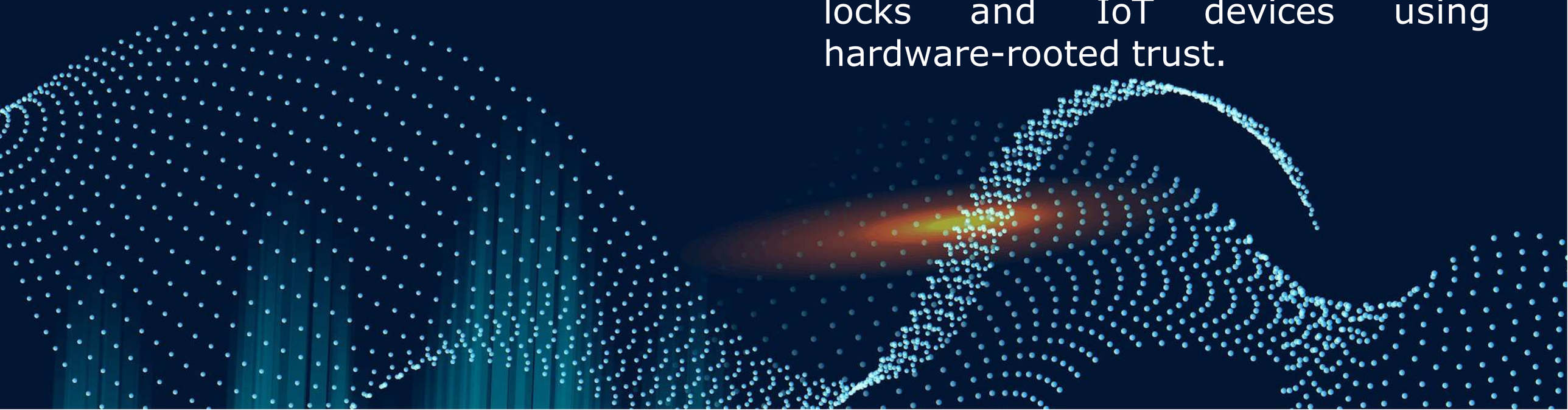
- Secura eliminates the need for backend servers or network calls.
- All cryptographic operations occur offline within the hardware.
- Ideal for environments with limited or no network connectivity.

# RSA PKCS/OAEP Encryption Protocol

- RSA encryption with PKCS/OAEP ensures robust data protection.
- Public-private key pairs used to secure device controls.
- Protects sensitive data and prevents unauthorized access.
- Encryption happens within the secure hardware enclave.

# Real-World Applications of Secura

- **UIDAI Authentication**: Secure, offline face authentication for Aadhaar using in-device PKI.
- **Mobile Banking**: Hardware-based encryption for secure transactions and payments.
- **Healthcare Devices**: Protect sensitive medical data and device access.
- **Smart Homes**: Secure control of locks and IoT devices using hardware-rooted trust.



# Conclusion

Secura is a hardware rooted security solution that stores encryption keys securely within the device, enabling offline, platform-agnostic protection. It offers robust key management and RSA encryption, ensuring secure control of devices, and is ideal for industries like smart homes, automobiles, and healthcare.